UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/406,910	09/24/1999	DAVID SCOTT HAYES	RIC-98-054	2067

25537 7590 10/06/2003

WORLDCOM, INC.
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2131	5

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/406,910	**Applicant(s)** HAYES, DAVID SCOTT	
	Examiner Syed Zia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 1999* .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas et al. (U.S. Patent 5,200,999).

3. Regarding claim 1 Matyas teaches and describes a method for authenticating transmitted data in real time, the method comprising the steps of:

- generating a master cryptographic key pair, including a first public key and a first private key, publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature based on the first public key, generating a disposable cryptographic key pair, including a second public key and second private key, generating a second certificate, the second certificate including the second public key and a second digital signature based on the second public key (col.12 line 28 to col.13line 9);

- publishing the second certificate, signing the data to be transmitted with a third digital signature by processing the data through a one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key, processing the received data through the one way hashing function to create a second hash value, decrypting the received third digital signature utilizing the second public key to obtain a third hash value, and verifying the authenticity of the data by comparing the second hash value to the third hash value (col.24 line 43 to col.26 line 14).

4. Regarding claim 13 Matyas teaches and describes a method for digitally signing data in real time, the method comprising the steps of:

- generating a master key pair including a first public key and a first private key, publishing a first certificate, the first certificate including the first public key and a first digital signature based on a certificate authority's key pair, generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair, generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair (col.12 line 28 to col.13line 9);

- dividing the data to be signed into packets, for each packet of data, computing a hash value based on the data in that data packet utilizing a one way hashing function, encrypting the hash value utilizing the second private key as the encryption key, and coupling each encrypted hash value with its corresponding data packet (col.24 line 43 to col.26 line 14).

5. Regarding claim 14 Matyas teaches and describes a method for verifying digitally signed data in real time, the method comprising
the steps of:

- processing the data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data, verifying the contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of along master key pair (col.24 line 43 to col.26 line 14);

- verifying the contents of a second certificate issued by the sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair, decrypting the digital signature portion of the digitally signed data utilizing the second public key to obtain a second hash value; and comparing the first and second hash values (col.19 line 58 to col.21 line 45).

6. Regarding claim 15 Matyas teaches and describes a method for digitally signing data in real time, the method comprising the steps of:

- generating a disposable key pair, the disposable key pair including a short public key and a short private key, publishing the short public key, dividing the data to be signed into packets, for each packet of data, computing a hash value based on the data in that data packet utilizing a one way hashing function, encrypting the hash value utilizing the short private key, and coupling each encrypted hash value with its corresponding data packet (col.7 line 18 to col.8 line 15, and col.19 line 58 to col.21 line 45).

7. Regarding claim 16 Matyas teaches and describes a method for verifying digitally signed data in real time, the method comprising the steps of:

- processing the data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data, decrypting the digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value, and comparing the first and second hash values (col.24 line 43 to col.26 line 14).

8. Claims 2-12 are rejected applied as above in rejecting claim 1. Furthermore, Matyas teaches an authentication the method for authenticating transmitted data in real time wherein –

- the step of generating a master key pair comprises creating long first public and private keys (col.7 line 18 to col.8 line 15);

- the first certificate further includes the identification of the sender and the identification of the certificate authority issuing the first certificate (col.2 line 47 to col.3 line 30);

- the first digital signature is produced by processing the data representing the identification of the sender, the identification of the certificate authority and the first public key through a one way hashing function to create a fourth hash value; and encrypting the fourth hash value utilizing a private key from the certificate authority to create the first digital signature (col.19 line 59 to col.21 line 45);

- the step of verifying the authenticity of the data comprising the first certificate (col.10 line 11 to line 32);

- the step of verifying the authenticity of the data comprising the first certificate comprises: decrypting the first digital signature to obtain a fifth hash value utilizing a public key issued by the certificate authority, processing the received data representing the identification of the sender, the identification of the certificate authority and the first public key through a one way hashing function to create a sixth hash value; and comparing the fifth and sixth hash values (col.19 line 58 to col.21 line 45);

- the step of generating a disposable cryptographic key pair comprises generating short second public and private keys (col.7 line 18 to col.8 line 15);

- the second certificate further includes the identification of the sender and the identification of the signing authority issuing the second certificate (col.2 line 47 to col.3 line 30);

- the second digital signature is produced by processing the data representing the identification of the sender, the identification of the signing authority and the second public key through a one way hashing function to create a seventh hash value; and encrypting the seventh hash value utilizing the first private key to create the second digital signature (col.19 line 59 to col.21 line 45);

- the step of verifying the authenticity of the data comprising the second certificate (col.10 line 11 to line 32);

- the step of verifying the authenticity of the data comprising the second certificate comprises decrypting the second digital signature to obtain an eighth hash value utilizing the first public key, processing the received data representing the identification of the sender, the identification of the signing authority and the second public key through a one way hashing function to create a ninth hash value; and comparing the eighth and ninth hash values (col.19 line 58 to col.21 line 45);

- dividing the data into packets and signing and authenticating each packet of data in accordance with steps (f) through (i) of claim 1 (col.9 line 35 to line 54).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-746-7240.

sz
September 30, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100